數聯資安

uSecure SIEM
事件管理•洞察•快速偵測

uSecure SIEM 資安事件管理系統是一款以日誌管理與分析為核心功能的 SIEM 產品。

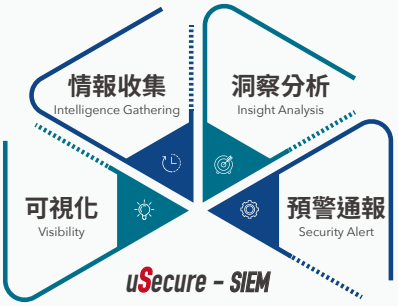
現今網路設備、伺服器與資安產品繁多，對 IT 人員來說，訊息完整的 Syslog Data 日誌軌跡保存與資安稽核調閱需求極為重要，資安法與個資法符規要求也與日俱增，uSecure SIEM能協助您集結所有事件管理與分析需求為一身，提供完整資安日誌分析、資安情資報表與關聯告警SIEM功能，使企業輕鬆掌握資安維運狀態。

- 資安設備系統日誌彙整收集
- 原始日誌保存稽核
- 異質紀錄綜合查詢
- 圖形化彙整分析
- 異常行為關聯警訊能力

產品特色：使資安事件管理更便捷、人性

協助企業保存資安事件軌跡，提升資安威脅管理、協同作業、與事件識別準確率

- 直觀視覺的儀表板與分析圖，資安事件可視化
- 日誌收容與情報收集，原始日誌保存稽核
- 內建關聯告警快篩功能，異常行為關聯警訊分析能力
- 洞察資安威脅、預警通報，並支援ISAC STIX情資交換格式



產品功能：洞察•威脅•告警

多樣化日誌收容及完整保存機制，確保資安事故管理完整性與可靠性

整合多樣日誌收容管道
提供多種收集能力，能有效整合應用系統及資安設備日誌輸出方式，達到日誌集中收容目的

原始日誌保存完整性機制
定時將原始日誌進行封裝加密保存，可透過特定機制校驗原始日誌封存檔案的完整性，確認檔案內容未遭竄改，確保事故調查的證據完整性及可靠

提供日誌字段全文檢索功能
可透過特定關鍵字的查找系統或設備的特定事件，查詢指令列支援複合運算，多層次過濾條件有助於縮減查找範圍與提升搜尋結果

內建角色權限功能

可依據角色設置操作功能權限，限制允許進行調閱的設備項目，並依各單位需求提供適切的權限進行日誌查閱，符合最小權限管理原則

視覺化儀表板及內建關聯告警通報，掌握資安維運狀態

具儀俵板綜合分析功能：

直觀視覺化分析圖，提供資安綜合分析儀俵板，可依需求自訂圖表項目，建立多面向維度的資安指標，快速掌握資安維運狀態

內建關聯告警快篩功能：

▲ uSecure 內建關聯規則

- 持續依內建關聯規則，篩檢侵入行為或可疑事件，進行告警通報，主動提供記錄供管理者 進行狀態分析及確認
- 提供電子郵件通知與呼叫Web API整合方式告警通報，並支援ISAC STIX情資交換格式
- 採已知特徵基礎及行為模式，自動偵測及發現異常，參考資安攻擊鏈各階段設置對應，制定精要的關聯機制，提供資安快篩功能，產生關聯告警，持續訂閱服務可獲得更新
- 內建支援多項資安設備整合，自動解析關鍵資訊做為儀表分析及關聯分析的分析因子，以指定管道收集尚未支援之項目，可進行完整日誌保存及全文關鍵字查閱

產品規格：

	1000 EPS以下	2000 EPS以下
硬體需求：	CPU：4 Cores RAM：16 GB Disk：3TB (SAS 7200rpm w/RAID 1)	CPU：8 Cores RAM：32 GB Disk：6TB (SAS 7200rpm w/RAID 1)
效能：	每日收集日誌儲存量: 10G 每日最大處理日誌量: 1000 EPS	每日收集日誌儲存量: 20G 每日最大處理日誌量: 2000 EPS
日誌保存：	可查詢日誌: 近180天 | 封存日誌: 365天	